ABSTRACT

The invention realizes a high-security cryptographic processing apparatus that increases difficulty in analyzing its key and a method therefor. In Feistel-type common-key-block cryptographic processing that repeatedly executes an SPN-type F-function having the nonlinear conversion section and the linear conversion section over a plurality of rounds, Linear conversion processing of an F-function corresponding to each of the plurality of rounds is carried out by linear conversion processing that applies square MDS (Maximum Distance Separable) matrices. The invention uses a setting that arbitrary m column vectors included in inverse matrices of square MDS matrices being set up at least in consecutive even-numbered rounds and in consecutive odd-numbered rounds, respectively, constitute a square MDS matrix. This structure realizes cryptographic processing whereby resistance to linear cryptanalysis attacks in the common-key-block cipher is improved.